Principles: Additional Safeguards for SCC Transfers

Companies of all sizes and in all industries rely on the ability to send data across international borders. In light of the July 16, 2020, decision by the Court of Justice of the European Union ("CJEU") in *Schrems II*, companies are considering appropriate measures to provide additional safeguards for data they transfer outside of the EU pursuant to Standard Contractual Clauses ("SCCs").

BSA | The Software Alliance has identified seven principles to guide companies adopting additional safeguards for EU data transfers. These principles focus on legal, technical, and organizational measures that companies can adopt to safeguard data in connection with government requests, such as requests from law enforcement or national security authorities. These principles are intended to help organizations develop specific safeguards that can supplement SCCs, and to provide a level of protection in addition to the measures already embodied in Commission-approved SCCs.

Companies adopting additional safeguards for SCC transfers must carefully assess the best way to implement these principles, based on the specific services they offer and the existing commitments they have already undertaken to safeguard personal data. These principles are accordingly intended to provide a strong foundation for companies adopting additional safeguards, while providing sufficient flexibility to enable companies to apply them on a case-by-case basis that reflects each company's particular services and the types of personal data they transfer.

Seven Principles for Additional Safeguards to Supplement SCCs:

1. **Establish Clear Processes for Responding to Government Requests.** Companies should provide businesses using their services (or individual users of the services, in the case of companies providing consumer-facing services) with clear information about how they review and respond to requests from government authorities.

2. **Require Government Requests to Be Narrow.** Companies should require government requests they receive to be targeted and to seek information about specific customers and accounts. Companies should construe government requests narrowly and should provide only the specific information sought by a request.

3. **Ensure Government Requests Are Lawful.** Companies should review government requests prior to disclosing personal data and should comply with a government request only if and to the extent it is valid.

4. **Tell Users About Government Requests.** Companies should notify their customers of government requests for the customers' information unless prohibited from doing so. For requests relating to business or enterprise customers, companies should attempt to redirect the request to the customer. Notice should be provided in a manner that aims to enable the customer to challenge the request or seek redress.

5. **Reject or Contest Invalid Government Requests.** If a company believes a request is invalid under applicable law, it should reject or contest the request, which may include using available mechanisms to challenge the request where appropriate or to seek to enable their customer to challenge the request.

6. **Adopt Technical Measures to Safeguard Data.** Companies should ensure that personal data is subject to appropriate technical safeguards, such as using encryption when technically feasible and appropriate given the type of data and services used.

7. **Be Transparent.** Companies should be transparent about the volume and nature of requests they receive from government authorities when legally permitted. When possible, companies should also be transparent about the total amount and general types of personal data disclosed in response to such requests.